Bugzilla ID: 601950
Bugzilla Summary: Turn on the code signing trust bit for the Thawte Primary Root CA

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	thawte
Website URL	http://www.thawte.com/
Organizational type	Commercial
Primary market / customer base	Thawte is a commercial CA with worldwide operations and customer base; it is a subsidiary of VeriSign, Inc.
CA Contact Information	CA Email Alias: practices@verisign.com CA Phone Number: 650.961.7500 Title / Department: Certificate Policy Manager

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	thawte Primary Root CA
Cert summary / comments	This root was included in NSS as per bug #407163, and the websites trust bit is currently enabled. This root is also enabled for EV. The current request is to enable the code signing trust bit.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=306736
SHA-1 fingerprint	91:C6:D6:EE:3E:8A:C8:63:84:E5:48:C2:99:29:5C:75:6C:81:7B:81
Valid from	2006-11-17
Valid to	2036-07-16
Cert Version	3
Modulus length / key length	2048
Test Website	https://www.thawte.com/
CRL URL	http://crl.thawte.com/ThawteEVCA2006.crl (NextUpdate: 7 days) CPS 4.4.9 CRL Issuance Frequency: For end-entity certs, the CRLs are issued "At Least Daily"
OCSP Responder URL	http://ocsp.thawte.com
CA Hierarchy	From bug #407163: The thawte Primary Root CA has two subordinate CAs, the thawte Extended Validation SSL CA and thawte Extended Validation SSL SGC CA, which issue the end entity EV certificates. Is this still accurate? Or does this root also have other intermediate CAs?

Externally operated subCAs	Does this root have any subordinate CAs that are operated by external third parties? If yes, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List any other root CAs that have issued cross-signing certificates for this root CA.
Requested Trust Bits	Requesting that the Code Signing trust bit be enabled. The Websites trust bit is currently enabled.
SSL Validation Type	EV Are DV or OV certs issued under this root?
EV policy OID(s)	2.16.840.1.113733.1.7.48.1
CP/CPS	Thawte Documents: http://www.thawte.com/repository CPS: http://www.thawte.com/cps/index.html
AUDIT	Auditor: KPMG Audit Type: WebTrust CA and WebTrust EV Audit Report & Management Assertions: https://cert.webtrust.org/SealFile?seal=527&file=pdf (2009.11.30)
Identity of Code Signing Subscriber	CPS Section 1.1, the table indicates that Code Signing Certificates are of High Assurance CPS Section 3.1.8.1 Authentication of the Identity of Organizational End-User Subscribers thawte confirms the identity of a Certificate Applicant for a High Assurance Server or Code Signing Certificate by: • Verifying that the organization exists through the use of at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization and • Confirming with an appropriate Organizational contact by telephone, postal mail, or a comparable procedure certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Organization is authorized to do so CPS Section 3.1.8.1: With respect to Starter PKI (SPKI) Customers, the identity confirmation process begins with thawte's confirmation of the identity of the Starter PKI Customer itself in accordance with this section. Following such confirmation, the Starter PKI Customer is responsible for approving the issuance of SSL Web Server and Code Signing Certificates within its own organization by ensuring that the server designated as the Subject of a SSL Web Server Certificate actually exists. Does this mean that other companies can issue Code Signing certs under this root?
Domain Name Ownership / Control	From bug #407163: Only EV SSL certificates are issued under the hierarchy rooted at the thawte Primary Root CA, with verification procedures per the EV guidelines. (See Appendix A1 of the CPS.) Is this still the case? Or are non-EV SSL certs also issued under this root? The EV procedures are described in Appendix A of the CPS. Appendix A.F.14 and 15: Verification of Applicant's Legal Existence and Identity Appendix A.F.16: Verification of Applicant's Physical Existence Appendix A.F.17: Verification of Applicant's Operational Existence Appendix A.F.18: Verification of Applicant's Domain Name

Email Address Ownership / Control	Not requesting email trust bit.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information. • 1.1 Long-lived DV certificates o • 1.2 Wildcard DV SSL certificates o • 1.3 Email Address Prefixes for DV Certs o • 1.4 Delegation of Domain / Email validation to third parties o • 1.5 Issuing end entity certificates directly from roots o • 1.6 Allowing external entities to operate subordinate CAs o • 1.7 Distributing generated private keys in PKCS#12 files o • 1.8 Certificates referencing hostnames or private IP addresses o • 1.9 Issuing SSL Certificates for Internal Domains o • 1.10 OCSP Responses signed by a certificate under a different root o • 1.11 CRL with critical CIDP Extension o • 1.12 Generic names for CAs o • 1.13 Lack of Communication With End Users o